REMARKS

Status of the Claims

Claims 1-15 are currently pending in the application. Claims 1, 3, 5 and 6 have been amended. No claims have been added. Support for foregoing amendments can be found throughout the specification, drawings, and claims as originally filed.

Claim 1 is in independent form. In the remarks that follow, Applicant first discusses independent claim 1 and then turns to the dependent claims of the claim set. The Examiner is respectfully requested to reconsider and withdraw the rejections in view of the amendments and remarks contained herein.

35 U.S.C. §103 Rejections

Claims 1-15 have been rejected under 35 U.S.C. 103(a) as being unpatentable over 3GPP TS 33.220 v6.0.0 (2004-03) 3rd Generation Partnership Technical Specification Group Services and System Aspects; Generic Authentication Architecture (GAA); Generic Bootstrapping architecture (Release 6) 22 March 2004 {herein after referred to as "3GPP"} in view of Faccin (PCT Pub. No. WO 03/014953). These rejections are respectfully traversed.

Independent claim 1 recites:

> A method for a roaming user to establish a security association with an application server in a visited network, wherein the roaming user has completed a mutual authentication with a Bootstrapping Server Function (BSF) that performs user identity initial verification in a generic authentication architecture in his home network, and obtained a Bootstrapping-Transaction Identifier (B-TID) assigned to him by the BSF, comprising:
>
> receiving a service request message, by the application server in the visited network, from the roaming user containing the B-TID;
>
> obtaining, by the application server in the visited network, the roaming user's user information comprising the user authentication results of the generic

authentication architecture in the roaming user's home network, wherein the user information is associated with the B-TID; and

establishing a security association with the roaming user, by the application server in the visited network, according to the user authentication results of the generic authentication architecture in the roaming user's home network.

In rejecting claim 1, the examiner asserts that 3GPP does not disclose that when the user roams in a visited network, after receiving a service request from the roaming user, the application server in the visited network establishes a security association with the roaming user after getting the user's information from the roaming user's home network. That is, 3GPP does not dislose these features: "receiving a service request message, by the application server in the visited network, from the roaming user containing the B-TID; obtaining, by the application server in the visited network, the roaming user's user information comprising the user authentication results of the generic authentication architecture in the roaming user's home network, wherein the user information is associated with the B-TID; and establishing a security association with the roaming user, by the application server in the visited network, according to the user authentication results of the generic authentication architecture in the roaming user's home network." However, the examiner asserts that Faccin has alrendy disclosed a feature employed for the same purpose wherein an application server in the visited network contacts the roaming user's home network in order to establish a security association.

Applicant has reviewed the cited portions and found no such teaching. Specifically, in Faccin page 6, lines 16-23, it is cited that "a Moble Node 100 sends its indentify and indications of the security association it needs to establish with a network entify via a connection that may include a wireless link to an Agent 110". In Faccin, page 10, line 10, it is cited that: " The agent 210 can determine that the Mobile Node 200 belongs to another network by analyzing the realm part of the NAI, for example". According to Faccin, the message from the Mobile Node includes its indentity. The Mobile Node's indentity is different from the B-TID assigned by the BSF in the independent claim 1. The independent claim 1 states receiving a service request message containing the B-TIA from from the roaming user. Therefore, Faccin does not disclose the feature "receiving a service

request message, by the application server in the visited network, from the roaming user containing the B-TID".

Furthermore, in Faccin page 9, line 24-25, it is cited that: "The Mobile Node 200 sends its identity through its NAI, for example, to the Agent 210 with the RAND1 and a MAC for integrity protection using the IK." According to Faccin, the information received by the Agent 210 is the Mobile Node's identity and some parameters. The identity of the Mobile Node and RAND1 and MAC are not the user authentication results of the generic authentication architecture in the roaming user's home network, and are different from the roaming user's user information in the independent claim 1. The roaming user's user information in claim 1 of the present invention comprising the user authentication results of the generic authentication architecture in the roaming user's home network, and what is important is that the roaming user's user information is associated with the B-TID. Therefore, Faccin does not disclose the feature "obtaining, by the application server in the visited network, the roaming user's user information comprising the user authentication results of the generic authentication architecture in the roaming user's home network, wherein the user information is associated with the B-TID;".

Furthermore, as disclosed at page 10, line 22-line 23 of Faccin, "the Subscriber database/Authentication Center 260, on behalf of the Mobile Node 200, starts the negotiations of the different parameters of a Security Association with the Agent 210." In Faccin, page 11, line 2-5, it is stated that "The Subscriber database/Authentication Center 260 will determine, from a database, which Security Association parameters are to be used, based on the parameters for Security Associations that the Mobile Node 200 supports." According to the Faccin, the security association is negotiated by the Subscriber database/Authentication Center and the Agent, and is determined by the Subscriber database/Authentication Center. The method of establishing the security association is completely different from the establishment in claim 1 of the present invention. In the claim 1, the application server in the visited network establishes a security association with the roaming user according to the user authentication results of the generic authentication architecture in the roaming user's home network. Therefore, Faccin does not disclose the feature "establishing a security association with the roaming user, by the application server in the visited network, according to the

user authentication results of the generic authentication architecture in the roaming user's home network."

In light of the foregoing, Applicant respectfully submits that claim 1 defines over the art cited by the Examiner. Because claims 2-15 depend from claim 1 directly or indirectly, they also define over the art cited by the Examiner.

CONCLUSION

In view of the foregoing, Applicant all claims now pending in this Application are in condition for allowance and issuance of a Notice of Allowance is respectfully requested.

If there are any other issues remaining which the Examiner believes could be resolved through a Supplemental Response or an Examiner's Amendment, the Examiner is respectfully requested to contact the undersigned at the telephone number indicated below.

The Commissioner is hereby authorized to charge any unpaid fees deemed required in connection with this submission or to credit any overpayment, to Deposit Account No. 04-0100.

Dated: July 6, 2009

Respectfully submitted,

By _____

Melvin C. Garner
Registration No.: 26,272
DARBY & DARBY P.C.
P.O. Box 770
Church Street Station
New York, New York 10008-0770
(212) 527-7700
(212) 527-7701 (Fax)
Attorneys/Agents For Applicant